UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	)	
	)	
v.	)	23-cr-118-SE-AJ-01
	)	
TYLER ANDERSON	)	

UNITED STATES' OBJECTION TO DEFENDANT'S SUPPLEMENT TO MOTION TO SUPPRESS AND ADDITIONAL ARGUMENTS

In addition to its prior objections to the defendant's Motion to Suppress (*see* ECF No. 21), the United States incorporates the following objections to the defendant's Supplement to the Motion to Suppress (ECF No. 24), and objections to new arguments made in his Reply brief (ECF No. 25). The search warrant was not overbroad in authorizing the search of the defendant's smartphone for evidence of the crime committed. Additionally, the search conducted was authorized by the clear language of the warrant. And even if the Court did find a Fourth Amendment violation, the good faith exception to the exclusionary rule should apply. Finally, the evidence collected from the defendant's phone should not be excluded by any Fifth Amendment violation.

A. Background

The United States incorporates the background set forth in its prior objection at ECF No. 21.

B. Discussion

The defendant makes several new arguments in support of his motion to suppress statements and evidence. Each of these new arguments, like his original contentions, should be rejected.

1. <u>The Search Warrant Was Sufficiently Particular.</u>

The defendant argues that the search warrant lacked particularity in that it did not limit the search of the defendant's cell phone to "text messages sent on December 8, 2023, or to a certain timeframe, even though the agents knew the alleged threat came via text on December 8, 2023." ECF No. 24 at 2. The defendant is wrong.

The Fourth Amendment requires that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement demands that a valid warrant: (1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized. *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999). This analysis is not strictly limited "to the four corners of the warrant" but also considers the circumstances of the warrant's issuance and execution. *United States v. Moss*, 936 F.3d 52, 59 (1st Cir. 2019).

Here, the warrant issued upon probable cause that the defendant used his Samsung Galaxy phone to send interstate threats in violation of 18 U.S.C. 875(c). The warrant specifically authorized the seizure of "evidence, contraband, or property designed for use, or used relating to violations of 18 U.S.C. § 875(c), those violations involving [defendant], and occurring on and after December 8, 2023," including the defendant's "Samsung Galaxy S10E with IMEI 35206610373174 and IMSI 311480604067856" and which was "used as a means to commit the violations described above". ECF No. 21-1 at Attachment B(1)-(1)(a). Reading these provisions together, the warrant authorizes the search of the defendant's cell phone for evidence of the crime. *See United States v. Kuc*, 737 F.3d 129, 132–33 (1st Cir. 2013) (in evaluating particularity, "a warrant's language must be read in context, such that "the 'general' tail of the

search warrant will be construed so as not to defeat the 'particularity' of the main body of the warrant."). This limitation, that the search is for evidence of the enumerated crime, is sufficient to satisfy the particularity requirement. *See United States v. Deschambault*, No. 2:19-CR-00187-JAW-1, 2022 WL 2916052, at *22 (D. Me. July 25, 2022) (rejecting a particularity challenge to a warrant authorizing the search of defendant's phone without limitation as to locations within the phone for evidence of the crime); *United States v. Alicea-Curras,* No. CR 22-511 (FAB), 2023 WL 6210882, at *4 (D.P.R. Sept. 25, 2023) (finding particularity requirement to be satisfied where search warrant language authorized search of defendant's cell phone for evidence related to the purported crime).

While the specific text messages described in the search warrant affidavit were evidence of the crime, there was other evidence of the crime that could also reside on the phone. Notably, the warrant also sought evidence in the form of "[r]ecords and information relating to threats to injure the person of another," "[r]ecords and information relating to the phone number 603-303-8914," and evidence of who "used, owned, or controlled" the phone including "email, email contacts, 'chat,' instant messaging logs, photographs, and correspondence." ECF No. 21-1, Attachment B(1)-(2). It is the nature of a cell phone that "[e]vidence can be found in multiple locations/applications" and "there are numerous ways in which a defendant can hide evidence of crimes in seemingly innocuous places." *United States v. Kormah*, No. CR 21-40012-TSH, 2023 WL 1490372, at *11 (D. Mass. Feb. 1, 2023).

In *Kormah*, the defendant challenged a search warrant that he claimed did not "limit the particular applications/locations on the phones to be searched, instead allowing law enforcement to forage throughout the entire phone accessing all available information." *Id.* The court found that the warrant was not overbroad, however, because the exact location of evidence within the

phone could not be known prior to the search and so "while law enforcement may be limited in that they c[ould] only look for and seize the information sought, they [we]re not limited as to where on the phone they may search for such information." *Id.*; *see also United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015) (rejecting a particularity challenge to a warrant authorizing a smartphone search for evidence of "Wire Fraud, Credit Fraud, [and] Identity Theft" where there was a basis to believe that evidence of the crime was on the phone, "but it was unclear as to the particular format in which the evidence existed."); *United States v. Palms*, 21 F.4th 689, 700 (10th Cir. 2021) (explaining that "in the electronic search context because search warrants typically contain few—if any—restrictions on where *within a computer* or other electronic storage device the government is permitted to search . . . [t]he reasonableness of the search method depends on the particular facts of a given case.") (quotations omitted) (emphasis in original).

The First Circuit's decision in *United States v. Corleto*, 56 F.4th 169, 176–77 (1st Cir. 2022), is also instructive. There, the court upheld a warrant authorizing the search of all cell phones and electronic devices found in the defendants' residence and vehicles that "may have been used as a means to commit the offenses described on the warrant" including production, possession, and transportation of child pornography. *Id.* Here, the warrant was even more targeted than in *Corleto* as the present warrant specifically identified one particular device, defendant's Samsung Galaxy phone, that was already shown to have been likely used to commit the crime. The need to search for evidence of the crime beyond just the specific text messages identified in the warrant application renders the warrant to be sufficiently particular.

The defendant focuses here on the alleged requirement that the search of the phone contain "temporal" limitations.[1] He cites three cases, *Abrams*, *Diaz,* and *Lafayette*, each of which involved warrants to search copious business, school, or medical records where the requests were not tailored to search for evidence any specific crime or to a period where evidence of wrongdoing might reasonably be found. *See United States v. Diaz*, 841 F.2d 1, 5 (1st Cir. 1988); *United States v. Abrams*, 615 F.2d 541, 544 (1st Cir. 1980); *Application of Lafayette Acad., Inc.*, 610 F.2d 1, 3 (1st Cir. 1979). But here, as explained above, the context shows that evidence related to the crime may be located on different applications and span different dates. There was thus no reasonable or discernable temporal limitation that the magistrate judge could have imposed within the scope of the warrant beyond the limitation she imposed, i.e., restricting the search to evidence related to the specific crime that occurred on a specific date. Evidence of this offense may have reasonably included text messages or other messages related to the defendant's threats that were dated earlier than the texts identified in the search warrant application. Consider, for example, earlier texts sent by the defendant to someone else showing his anger at one of the victims. Such texts would be evidence of the threat offense. The warrant also recognized that messages on the phone from earlier dates would be relevant to show who used or controlled the phone at any given time.

At what point should the magistrate judge have prophylactically declared evidence to be too far removed from December 8, 2023 to be excluded from the authorized search? The

[1] In this and other arguments, defendant relies heavily on the Supreme Court's 2014 decision in *Riley v. California*. The government recognizes the significant privacy interest in cell phones that the *Riley* decision noted, but that case stands for the proposition that a warrant is generally required before searching a cell phone, including when the phone is seized incident to arrest. *See* 573 U.S. 373, 401 (2014). Here, the government is not contesting that a warrant was required to search the phone—which is precisely why such a warrant was secured prior to the seizure and search of the defendant's phone.

defendant provides no clear answer—and none exists under these circumstances. *See Corleto*, 56 F.4th at 176 (defendant "invokes no authority for the implied proposition that a warrant affidavit need predict with omniscient precision exactly where on the premises the evidence to be seized may be located. And for good reason: The authority is to the contrary.").

The defendant also cites to *United States v. Holcolmb*, from the Western District of Washington which found a search warrant to be overbroad. 639 F. Supp. 3d 1142, 1145 (W.D. Wash. 2022). But that case is inapposite as it involved a search for a specific video, which was recorded at a known time on a known date. *Id.* at 1144. Here, as detailed above, while the warrant sought evidence related to a crime committed on a known date, the dates and locations within the phone of all relevant evidence related to that crime were not known. Finally, the defendant cites to a 10th Circuit case, *United States v. Russian*, which found a search warrant for "cell phones that could be used to facilitate the crimes" to be overbroad. 848 F.3d 1239, 1243 (10th Cir. 2017). But the facts of *Russian* are not analogous to the present case, and in fact, the *Russian* holding supports a finding of particularity here. In *Russian*, the warrant failed because it did not identify the specific devices to be searched. *Id.* Here, the warrant included the exact model and device identifier of the phone to be seized – and probable cause to show that that specific device was used to carry out the crimes. Moreover, the *Russian* court explained that "warrants may pass the particularity test if they limit their scope either to evidence of specific federal crimes or to specific types of material." *Id.* at 1245 (internal quotations omitted). This is precisely what the warrant here did. It was not overbroad.

2. <u>The Search of the Defendant's Smartphone Was Within the Scope of the Warrant.</u>

In his Reply brief, the defendant also introduces a new argument that the search of the defendant's Samsung Galaxy phone exceeded the scope of the warrant. This argument simply is

incorrect. As explained in the prior section, the language of the search warrant could not be clearer in its authorization to search the phone for evidence of the crime. Each of defendant's specific arguments on the scope of the search fail.

First, the defendant argues that while the warrant authorized the seizure of the phone, it did not authorize its search. ECF No. 25 at 5. That is incorrect for the reasons explained in the prior section. The warrant authorized the seizure of the phone along with "evidence, contraband, or property … relating to" the violations. ECF No. 21-1, Attachment B(1)-(1)(a). As explained above, these provisions must be read in tandem and together authorize the search of the phone for evidence of the crime. *See Kuc*, 737 F.3d at 132–33. There is no question that evidence on the phone was subject to seizure.

Second, defendant argues that the provision authorizing seizure of "records and information relating to threats to injure the person of another" did not permit the search of the phone because the warrant describes "records and information" as "including any form of computer or electronic storage (such as hard disks or other media that can store data)" and he separately argues that "computer or electronic storage" does not include a cell phone. ECF No. 25 at 5-6 (citing ECF No. 21-1 at 6-7). This is plainly wrong as the warrant defines "computer" to include "mobile phones" and so "computer storage" would certainly include data stored on the phone. Moreover, "all forms of creation or storage" would also encompass information located on and stored in the phone. Finally, any question of whether "computers or storage media" includes the phone itself is answered by language of the warrant authorizing seizure of "[c]omputers or storage media used as a means to commit the violations described above, *namely Samsung Galaxy S10E* with IMEI 35206610373174 and IMSI 311480604067856." ECF No. 21-

1, Attachment B(1)(a) (emphasis added). The phone itself is explicitly described as "computer[] or storage media."

Third, the defendant argues that the warrant's permission to seize "'chat,' correspondence, and instant message logs" for evidence of who used, owned, or controlled the phone did not extend to permission to search for these items on the defendant's phone. The defendant asserts that "text messages do not constitute evidence of who used, owned, or controlled a cell phone at any given time, as they do not require their author to identify themselves." ECF No. 25 at 6. While it's true that text messages do not require the author to self-identify, it is also apparent that the content of a text message contains evidence of who sent that text message and provides relevant context, information, and evidence of who used the phone at a given time. The warrant's permission to seize information about who used the phone would extend permission to search many areas of the phone, including text messages.

Finally, the defendant argues that permission to review "electronic storage media and electronically stored information" to locate evidence does not authorize the search of the phone. For the reasons set forth above and based on the plain language of the warrant and common understanding of the words, "electronic storage media and electronically stored information" would include the contents of a mobile phone.

Contrary to each of the defendant's arguments, the warrant in fact sets forth numerous separate bases upon which the search of the defendant's phone was authorized.

3. <u>The Good Faith Exception to the Exclusionary Rule Applies.</u>

Even if the warrant were invalid, which it is not, or the search of defendant's phone exceeded the scope of the warrant, which it did not, the evidence from the phone would still be admissible under the good faith exception to the exclusionary rule. The good faith exception

applies "when government agents rely on a warrant in objective good faith and in the interest of justice suppression is generally inappropriate." *United States v. Woodbury*, 511 F.3d 93, 99 (1st Cir. 2007). The good faith exception does not apply where an agent's good faith reliance on a warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or where the warrant is "so facially deficient—*i.e.* in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* (quoting *United States v. Owens,* 167 F.3d 739, 745 (1st Cir.1999)). It is undisputed here that the warrant was based on probable cause. It is also clear, for the reasons set forth above, that the warrant facially authorized the search of the phone with the limitation that the search be for evidence of the specific crime. Finally, the agents carried out the search within the scope of the warrant. Even if the warrant was invalid here, the court should conclude that the agents acted in good faith in relying on it. *See Kuc,* 737, F.3d at 134 ("the warrant, read comprehensively and in context, was not so facially deficient ... that the executing officers could not reasonably presume it to be valid") (quotations omitted); *United States v. Quiñones*, No. 19-309 (ADC), 2019 WL 8060625, at *5, (D.P.R. Dec. 9, 2019) (despite "defects in the warrant application," agents acted in good faith reliance on a search warrant which "was not facially deficient as it identified Defendant's cellphone as the item to be searched"); *see also Holcomb*, 639 F. Supp. 3d at 1147 (applying the good faith exception); *Russian*, 848 F.3d at 1248 (same).

4. The *Patane* Rule Extends to Cell Phones.

The defendant also argues that the rule set forth in *United States v. Patane,* 542 U.S. 630 (2004), namely that a voluntary statement made in violation of *Miranda* does not result in the exclusion of physical evidence which might be the fruits of that statement, should not include

evidence located on a cell phone.[2] ECF No. 25 at 9-10. The government previously cited *United States v. Billings*, No. 2:17-CR-122-NT, 2018 WL 283244 (D. Me. Jan. 3, 2018), *United States v. Hernandez*, No. 18-CR-1888-L, 2018 WL 3862017 (S.D. Cal. Aug. 13, 2018), and *United States v. Mendez-Bernal*, No. 319CR00010TCBRGV, 2020 WL 6495109 (N.D. Ga. July 22, 2020), *report and recommendation adopted,* No. 3:19-CR-10-TCB, 2020 WL 5494728 (N.D. Ga. Sept. 11, 2020), each of which applied the *Patane* rule to admit evidence from cell phones. *See* ECF 21 at 7. These cases are each directly on point here. As his support for a contrary proposition, the defendant cites a single case, *United States v. Djibo*, 151 F. Supp. 3d 297, 309 (E.D.N.Y. 2015). But while *Djibo* does cite *Riley* in recognizing a heightened privacy concern in the context of cell phones, the case rests on a finding that a subsequent cell phone search was tainted by a prior warrantless *search* of that same cell phone. *Id.* It applied the exclusionary rule to illegal fruits of a *Fourth Amendment* violation—not a *Miranda* violation. *Id.* Defendant has no authority that *Patane*'s reach does not extend to cell phones in the absence of a separate Fourth Amendment violation. That makes sense. The *Patane* rule is based on the nature of the violation, not the nature of physical evidence seized. The court should follow the *Billings*, *Hernandez*, and *Mendez-Bernal* cases which account for years of post-*Riley* jurisprudence and are legally and factually analogous to the present case.[3]

5. <u>The Inevitable Discovery Doctrine Applies.</u>

[2] The defendant also argues that his act of providing his passcode was not voluntary. *See* ECF 25 at 8-9. The government refers to it's argument to the contrary at ECF No. 21 at 5-7.

[3] Defendant cites to *United States v. Booker*, but that case does not apply here because, just as in *United States v. Clark*, No. CR 3:22-30012-MGM, 2023 WL 4706521 (D. Mass. July 21, 2023)—which defendant cited in his original motion to suppress, the defendant's statements to law enforcement were presumed to be involuntary because they followed an invocation of the right to counsel. 561 F. Supp. 3d 924, 941-42 (S.D. Cal. 2021). Here, it is undisputed that no such invocation occurred prior to defendant providing his passcode.

Finally, defendant argues that the inevitable discovery doctrine should not apply because the warrant was invalid, the search exceeded the scope of the warrant, and therefore the contents of the phone could not have been discovered lawfully. For the reasons set forth above and in the government's prior objections (ECF 21 at 8), the inevitable discovery doctrine should apply. The warrant was not overbroad; it authorized the search of defendant's phone; agents acted in good faith reliance on the warrant; and evidence at the hearing will show that the agents could have accessed the contents of the phone without defendant's passcode.

C. Conclusion

For the reasons stated herein and in the government's prior objections (ECF No. 21) the motion to suppress should be denied.

Respectfully submitted,

JANE E. YOUNG
UNITED STATES ATTORNEY

Dated: March 6, 2024

By: /s/ Matthew P. Vicinanzo
Charles L. Rombeau
Matthew P. Vicinanzo
Assistant United States Attorneys
53 Pleasant Street, 4th Floor
Concord, NH 03301
(603) 225-1552
charles.rombeau@usdoj.gov
matt.vicinanzo@usdoj.gov